REMARKS

Reconsideration of the application in light of the amendments and the following remarks is respectfully requested.

A. Status of the Claims

Claims 1-15 are now pending in the application. The Examiner is respectfully requested to reconsider and withdraw the rejections in view of the remarks contained herein.

B. Overview of the Faccin Reference

Faccin (PCT Pub. No. WO 03/014953) discloses a negotiation to establish a Security Association between the Mobile Node or terminal 200 and the Agent 210 in the environment of Fig 2. The Mobile Node 200 sends a **request message** containing its identity with RAND1 and a MAC to the Agent 210 (Page 9, Lines 24-26). The Agent 210 forwards the identity, RAND1 and the MAC to the Visited GW 230 (Page 10, Lines 4-5). The Visited GW 230 then transmits the identity, RAND1 and the MAC, to the Home Network GW 240 (Page 10, Lines 13-14). The Home GW 240 then forwards the message to the Subscriber database/Authentication Center 260 (Page 10, Lines 17-18). The Subscriber database/Authentication Center 260 verifies the correctness of the MAC and, on behalf of the Mobile Node 200, starts the negotiation of the different parameters of a Security Association with the Agent 210 (Page 10, Lines 21-25). The Subscriber database/Authentication Center 260 will determine from a database, which Security Association parameters are to be used (Page 11, Lines 2-3), and will send the parameters to the Agent 210 (Page 11, Lines 12-14; Fig 3, 4).

To sum up, in the Faccin, **the Mobile Node 200 was verified after the Visited GW received the request message,** i.e. the Visited GW 230 forwards the request message from the Mobile Node 200 to the Subscriber database/Authentication Center 260 through the Home GW 240, then the Mobile Node 200 is verified by the Subscriber database/Authentication Center 260. What

the Visited GW 230 receives from the subscriber database/Authentication Center 260 **is only Security Association parameters**.

C. Overview of the Invention

Claim 1 of the present invention discloses a method to establish a security association between a roaming user and a visited network. The **roaming user has already completed a mutual authentication with a Bootstrapping Server Function ("BSF")** of the generic association architecture in the home network **before the application server in the visited network receives a service request message**, and obtains a Bootstrapping-transaction Identifier ("B-TID") from the BSF. Therefore, when the visited network receives a request message from the roaming user to establish a security association, the **visited network can directly obtain the user authentication results** of the generic authentication architecture in the home network. Due to the fact that the roaming user has already been authenticated by the home network, the visited network can then establishes the security association **without the need to authenticate the roaming user after receiving the request**.

D. 35 U.S.C. §103 Rejections

Claims 1-15 have been rejected under 35 U.S.C. 103(a) as being unpatentable over 3GPP TS 33.220 v6.0.0 (2004-03) 3rd Generation Partnership Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping architecture (Release 6) 22 March 2004 {herein after referred to as **"3GPP"**} in view of Faccin (PCT Pub. No. WO 03/014953).

Applicant respectfully states that 3GPP does not specifically disclose the roaming or visiting server elements of the claims as follows:

*wherein **the roaming user has completed a mutual authentication** with a Bootstrapping Server Function (BSF) that performs user identity initial verification in a generic authentication*

architecture in his home network, and ***obtained a Bootstrapping-Transaction Identifier (B-TID)*** *assigned to him by the BSF*

receiving a service request *message, by the application server in the visited network, from the roaming user containing the B-TID;*

obtaining, by the application server ***in the visited network****, the roaming user's user information comprising the user authentication results of the generic authentication architecture in the roaming user's home network, wherein the user information is* ***associated with the B-TID****;*

establishing a security association with the roaming user, by the application server ***in the visited network****, according to the user authentication results of the generic authentication architecture in the roaming user's home network.*

The features recited in the claim 1 refer to the home network and the visited network in which there are interactions between the home network and the visited network. However, 3GPP only refers the home network, so the method in the home network in the 3GPP can't disclose both the technical features in the home network and the visited network. Therefore, 3GPP does not disclose all the technical features recited above.

Furthermore, Faccin also fails to disclose these features. The Examiner asserted that: "In actuality the (page 6, lines 16-23) point outs out what is sent is in fact the identity and indications of the security associations (i.e. obviously a transaction identifier)" and "3GPP…further defines a transaction identifier as a key identifier (i.e. integrity key "IK")". Applicant respectfully disagrees.

The page 6, lines 16-23 of Faccin discloses that "a Mobile Node 100 sends its identity and indications of the Security Association it need to establish with a network entity…" Faccin **does not disclose that the identity and indications are assigned by the home network**.

Furthermore, section 4.3.7 of the 3GPP discloses that the "Transaction identifier shall be used to bind the subscriber identity to the keying material in Ua, Ub and Zn interfaces." Thus, it is obvious that the transaction identifier is not a key. Therefore, the **Mobile Node's identity and**

indications cannot be equal to the B-TID which is assigned to the roaming user by a BSF in the home network after the authentication, and **the transaction identifier in the 3GPP (primary reference) cannot be equal to the integrity key "IK"**.

The B-TID is a completely different concept from the identity or the indications or the integrity key. Therefore, Faccin does not disclose the feature "receiving a **service request message**, by the application server in the visited network, from the roaming user **containing the B-TID**".

Furthermore, "the SA negotiation and 'FINAL RESULTS' directed toward V-GW" in Faccin are different from "the information comprising the user authentication results of the generic authentication architecture in the roaming user's home network, wherein the user information is associated with the B-TID".

As described above, in the Faccin **the Mobile Node 200 was verified after the Visited GW received the request message.** But in claim 1 of the present invention, as described in the ***Overview of the Invention***, the roaming user **has been authenticated** by a BSF in the generic authentication architecture in the home network **before the application server in the visited network received a request message**, so the application server in the visited network can **obtain the user authentication results in the visited network directly from** the generic authentication architecture in the home network according to the B-TID.

The generic authentication architecture is common knowledge to the skilled person in the field. For example, the title of 3GPP TS 33.220 introduces the "Generic Authentication Architecture (GAA)," and 3GPP TR 31.919 V1.2.0 (2003-12) defines the GAA (section 4). The GAA includes a BSF, i.e. Generic Bootstrapping Architecture, is described in the 3GPP 33.220. **Therefore, the generic authentication architecture in the claim 1 has a definite architecture to a person skilled in the field.** Obviously, the generic authentication architecture including a BSF in claim 1 is different from Faccin's network architecture. The user authentication results of the

generic authentication architecture in the roaming user's home network, which are verified by the BSF, are also different from "the SA negotiation and 'FINAL RESULTS'" in the Faccin.

What is more, while the application server in the visited network is associated with the B-TID, in the present invention it is obvious that Faccin does not disclose this technical feature because in Faccin there is no B-TID.

Moreover, as described in the *Overview of the Faccin Reference*, **what the Visited GW 230 receives from the subscriber database/Authentication Center 260 is only Security Association parameters**. However, in claim 1, what the application server in the visited receives the user authentication results. To a person skilled in the field, the security association parameters is different from the authentication results.

Thus, it can be conclued that Faccin fails to disclose "obtaining, by the application server in the visited network, the roaming user's user information comprising the user authentication results of **the generic authentication architecture in the roaming user's home network**, wherein **the user information is associated with the B-TID**" as recited in claim 1 of the present invention.

Additionally, according to the *Overview of the Faccin Reference*, Faccin discloses that the **Subscriber database/Authentication Center 260**, on behalf of the Mobile Node 200, **starts the negotiations of the different parameters of a Security Association with the request from the Agent 210**, and then the Subscriber database/Authentication Center 260 sends the parameters to the Agent 210.

In the claim 1 of the present invention, the **application server in the visited network establishes a security association with the roaming user** according to the user authentication results of the generic authentication architecture in the roaming user's home network. As described above, the application server in the visited network can establish the security association with the roaming user if the application server in the visited network can identify that the roaming user has

been authenticated by the BSF of the generic authentication architecture in the home network. Therefore, Faccin does not disclose the feature "establishing a security association with the roaming user, by the application server in the visited network, according to the user authentication results of the generic authentication architecture in the roaming user's home network."

For at least the foregoing reasons, claim 1 should be allowable over 3GPP and Faccin.

Claim 2 depends from claim 1, and thus requires all of the elements recited in claim 1.

Moreover, Applicant respectfully traverses the Examiner's position that the 3GPP (section 4.4.3; section 4.3.7) discloses "the application server in the visited network sending a query message **to an authentication entity** in the local network to inquire about the user information associated with the B-TID" and "**the authentication entity** which received the message finding out the home network to which the user belongs according to the B-TID in the message." The 3GPP discloses that "**BSF** to fetch the required authentication information and subscriber profile information from the HSS" and "**NAF** shall be able to detect the home network." It is obviously that **it is the same entity, i.e. authentication entity**, that receives the query message and finds out the home network in the claim 2. However, in the 3GPP, there are **two different entities, i.e. BSF and BAF**, fetch information and detect the home network.

Furthermore, 3GPP does not disclose that a roaming users' information is obtained while in a visiting network or that the application server is in a visiting network. As described above, the generic authentication architecture in claim 2 is different from the network architecture in the Faccin. Therefore, the features disclosed by Faccin could not be included within the technical disclosure document of 3GPP.

Accordingly, claim 2 should also be allowable over 3GPP and Faccin.

Claims 3-15 should be allowable at least due to their dependence from claim 1. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejection of claims 1-15 under 35 U.S.C. 103(a).

CONCLUSION

In view of the foregoing, Applicant believes all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested. Applicant does not acquiesce to any argument not specifically addressed herein. Rather, Applicant believes the amendments and arguments contained herein overcome all rejections presented.

If there are any other issues remaining which the Examiner believes could be resolved through a Supplemental Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at the telephone number indicated below.

Dated: December 11, 2009

Respectfully submitted,

By _____

Melvin C. Garner
Registration No.: 26,272
DARBY & DARBY P.C.
P.O. Box 770
Church Street Station
New York, New York 10008-0770
(212) 527-7700
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant